SECURE SPLIT TESTFOR PREVENTING IC PIRACY BY UN-TRUSTED FOUNDRY AND ASSEMBLY.

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF TECHNOLOGY

IN

VLSI DESIGN AND EMBEDDED SYSTEM

BY

HANUMANTHA RAO GORREPATI

213EC2197

Under the Guidance of

PROF. KAMALA KANTA MAHAPATRA

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA

ODISHA, INDIA. 769008

2013 – 15

SECURE SPLIT TEST FOR PREVENTING IC PIRACY BY UN-TRUSTED FOUNDRY AND ASSEMBLY.

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF TECHNOLOGY

IN

VLSI DESIGN AND EMBEDDED SYSTEM

BY

HANUMANTHA RAO GORREPATI

213EC2197

Under the Guidance of

PROF. KAMALA KANTA MAHAPATRA

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA

ODISHA, INDIA. 769008

2013 – 15

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY

ROURKELA

Certificate

This is to certify that the thesis report entitled

SECURE SPLIT TEST FOR PREVENTING IC PIRACY BY UN-TRUSTED FOUNDRY AND ASSEMBLY.

Submitted by

MR. HANUMANTHA RAO GORREPATI

Bearing roll no. **213EC2197**

In partial fulfillment of the requirements for the award of

MASTER OF TECHNOLOGY

In

VLSI DESIGN AND EMBEDDED SYSTEM

During session 2013-15 at National Institute of Technology, Rourkela, is an authentic work carried out by him under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other university/institute for the award of any degree or diploma.

Prof. Kamala Kanta Mahapatra
Department of ECE,
National Institute of Technology,
Rourkela – 769008.

Date: June 1st, 2015

DEDICATED TO MY PARENTS

MR. ANJAIAH GORREPATI

MRS. PITCHAMMA GORREPATI

AND MY BROTHER

MR. VEERANJANEYULU GORREPATI

WHOSE INSPIRATIONS HAVE ALWAYS MOTIVATED ME TOWARDS MY GOAL.

LIST OFCONTENTS

ACKNOWLEDGEMENT

It was almost twenty-two months since I officially got associated with NIT Rourkela for my post-graduation studies. And what this entire period of time have been; packed with profound knowledge and splendid experience, hard work for fun, enjoyment and frustration, teamwork and friendship. At the end of this wonderful period of time, I wish to give away a vote of thank to all the people who held my hand for pursuing an M. Tech degree.

First and foremost, I would like to express my sincerest gratitude to my research advisor Prof. K. K. Mahapatra, for his guidance, advice and support throughout my thesis work. He inspired, motivated, encouraged and gave me full freedom to do my work with proper suggestions throughout my research work. I am also greatly indebted to Mr. Sudeendra Kumar, a Ph.D. scholar at NITRKL, for introducing the exciting topics in this domain to me, an infant M. Tech student who started journey on unknown paths in this space. Without his knowledge and priceless guidance for this research, boundless efforts and patience, and long lasting technical discussions, this research would have never been fruitful. Many thanks to both of you for such unmatched support.

I express my wholehearted gratitude to Prof. D. P. Acharya, Prof. P. K. Tiwari, Prof. A. K. Swain, and Prof. N. Islam for their thoughtful teaching and suggestions during my courses in M. Tech and making available all necessary facilities and infrastructure for studies. I am also thankful to all research scholars in VLSI lab and all other labs for maintaining the lab, availing access to the same 24×7 and creating a vibrant atmosphere for research.

Away from home in a distant land, the people who constantly support and encourage a person are his friends. I am utmost greatful to my friends S. Anil Kumar, Ch. Rakesh, P. Siddhartha, Ch. Krishna Reddy and S. Sailaja, and here at NIT Rourkela. Apart from the regular

education from my professors, I have learnt many things from my friends. I would like to express my thanks to all of them for making these two years a fantabulous journey.

Finally, I thank GOD for blessing me with a loving and supporting parents and my younger brother as I would not have even dreamed of pursuing higher education without their love, affection and support. My parents are my first teachers after I came to this world.

Hanumantha Rao. Gorrepati

ABSTRACT:

In the era of globalization, integrated circuit design and manufacturing is spread across different continents. This has posed several hardware intrinsic security issues. The issues are related to overproduction of chips without knowledge of designer or OEM, insertion of hardware Trojans at design and fabrication phase, faulty chips getting into markets from test centers, etc. In this thesis work, we have addressed the problem of counterfeit IC's getting into the market through test centers. The problem of counterfeit IC has different dimensions. Each problem related to counterfeiting has different solutions. Overbuilding of chips at overseas foundry can be addressed using passive or active metering. The solution to avoid faulty chips getting into open markets from overseas test centers is secure split test (SST). The further improvement to SST is also proposed by other researchers and is known as Connecticut Secure Split Test (CSST). In this work, we focus on improvements to CSST techniques in terms of security, test time and area.

In this direction, we have designed all the required sub-blocks required for CSST architecture, namely, RSA, TRNG, Scrambler block, study of benchmark circuits like S38417, adding scan chains to benchmarks is done. Further, as a security measure, we add, XOR gate at the output of the scan chains to obfuscate the signal coming out of the scan chains.

Further, we have improved the security of the design by using the PUF circuit instead of TRNG and avoid the use of the memory circuits. This use of PUF not only eliminates the use of memory circuits, but also it provides the way for functional testing also. We have carried out the hamming distance analysis for introduced security measure and results show that security design is reasonably good.

Further, as a future work we can focus on:

- Developing the circuit which is secuered for the whole semiconductor supply chain with reasonable hamming distance and less area overhead.

LIST OF FIGURES:

LIST OF TABLES:

LIST OF SYMBOLS AND ABBRIVATIONS

Thefollowingisthelistofabbreviationsthatareencounteredinthisthesis.

AES	Advanced Encryption Standard
ASIC	ApplicationSpecific IntegratedCircuits
ATE	AutomaticTestEquipment
ATP	AutomaticTestPatterns
ATPG	AutomaticTestPatternGeneration
CAD	Computer Aided Design
CMOS	ComplementaryMetalOxide Semiconductor
CSST	Connecticut Secure Split Test
DC™	Design Compiler
DFT	DesignforTestability
DUT	DesignunderTest
ECID	Electronic Chip ID
FSM	Finite State Machine
HDL	HardwareDescriptionLanguage
IC	IntegratedCircuit
IP	IntellectualProperty
LFSR	LinearFeedbackShiftRegister
LSSD	Level Sensitive Scan Design
OCM	Original chip manufacturer
PCB	Printed Circuit Board

PDF	PathDelayFault
PRNG	Pseudo Random Number Generator
PUF	Physical UnclonableFunction
RTL	RegisterTransferLogic
S-A-0/1	Stuck-At-1/0
SAF	StuckAtFault
SPF	STIL Procedure File
SST	Secure Split Test
STA	Static Timing Analysis
TRNG	True Random Number Generator
TSMC	Taiwan Semiconductor Manufacturing Company
VCS	Verilog Compiler Simulator
VLSI	Very Large Scale Integration

PUBLICATION

- **Hanumantha Rao Gorrepati,** Sudeendra Kumar and K.K.Mahapatra, "A Novel PUF based SST to prevent Distribution of Rejected ICs from Untrusted Assembly" (communicated).

1. CHAPTER 1: OVERVIEW

1.1: INTRODUCTION

1.2: MOTIVATION

1.3: RESEARCH OBJECTIVE

1.4: CONTRIBUTION OF THE DISSERTATION

1.5: ORGANISATION OF THE THESIS

1.1. INTRODUCTION:

It is a human tendency to achieve more perfection in every field including electronics. So every time technology of electronic devices is increasing. These electronic devices are made of semiconductor materials which have different electronic properties at different conditions like temperature, doping, etc. Integrated circuits are the circuits which will have thousands of transistors are fabricated in a single chip, as the technology increases density of integrated circuits increases.

There are three design methodologies for the manufacturing of these integrated circuits. 1) Full custom design 2) semi-custom design 3) ASIC design. Full custom design means each transistor in the design is personally designed and all these are integrated and routed manually. In semi-custom design some of the devices are taken from the standard libraries and all these are integrated. ASIC design was a design that is designed specifically for a particular circuit.

Hardware security issues:

There are many hardware security issues in semiconductor industry [17]. This security issue includes side channel attacks, reverse engineering, IP piracy, counterfeiting, IC overbuilding, Hardware Trojan insertion and power analysis. Among the following security issues we are working on the problem of counterfeiting. This counterfeiting of ICs includes reusing of chips, overproduction of chips and sending out of spec ICs into the market.

In this thesis, we are concentrating mainly on controlling the out of spec ICs to enter into the market. There are already existing solutions to overcome the counterfeits [12] [13] [14].

1) Secure Split Test: this paper gives the solution for preventing IC counterfeiting by including IP owner in the test procedure. Here only after giving the secret key ICs are

unlocked and those ICs will give correct functionality and those results will be scanned only by the IP owner and he will decide the PASS/FAIL of the chip.

2) Connecticut Secure Split Test: This paper overcomes the disadvantages of SST by the same researchers. Disadvantages of SST are complex communication between IP owner and testing centre. Here communication between IP owner and the foundry is decreases and security is increases by inserting scrambling block into the testing procedure.Detailed description of these Anti-counterfeiting methods is described in the following chapter 2 Literature Review.

1.2. MOTIVATION:

Since the complexities in the semiconductor industry is increases and many fabrication companies can't bear the manufacturing cost of the IC. So many fabless companies outsource their devices. Here at the manufacturing centre each IC is tested on testing equipment called Automatic Test Equipment (ATE). This equipment is costly, so testing cost is high.

Because of un-trusted foundry and assembly, two types of IC counterfeits will occur. 1) Overproduction of chips than they are ordered. 2) Sending out of spec ICs or partially passed ICs into the market. Because of these counterfeits there may be financial loss to the original chip manufacturer (OCM) and if these faulty chips have entered into the market then the reputation of the company will be decreases.

To overcome these drawbacks, many anti-counterfeit techniques have been proposed. All these methods had overcome some of the counterfeits. Previously, two methods are proposed called SST and CSST [12] [13] to overcome one of the main drawbacks called shipping out of spec ICs into the market.

1.3. **RESEARCH OBJECTIVE:**

Since each manufacturing IC must be tested and counterfeit techniques has been increased. According to the survey of Alliance group of Gray Market 10 percent of electronics in the market are counterfeits.

The Main aim of this research is to increase the security of the design with less area and power overhead. This security is mainly because of untrusted foundry and assembly during the testing of IC.

1.4. **CONTRIBUTION OF THIS DISSERTATION:**

In this thesis, we have proposed and designed a novel PUF based SST. Here we are implementing the SST by using Physical Unclonable Functions (PUFs) which is used to generate the numbers randomly. In this we have used RSA, PRNG and Scrambler blocks with reduced test time and area overhead. Arbiter PUF is used which will have good features like reliability, uniformity.

1.5. ORGANISATION OF THE THESIS:

Following an overview, rest of the dissertation is structured as follows

Chapter2: This chapter describes the fundamentals of VLSI testing. It defines various types of tests that are using in present days. Among those tests it mainly concentrates on test for manufacturing defects, their modelling and discussed about literature review.

Chapter3: This chapter gives detailed view of various industry tools for modelling stuck-at faults (SAF).

Chapter4: This chapter details various SST structures that are proposed to overcome the different counterfeits.

Chapter5: This chapter gives the overview of proposed novel PUF based SST by improving the drawbacks of previous SST structures.

Chapter6: This chapter describes about various PUF structures and finally about the Arbiter PUF structure which uses in this thesis.

Chapter7: This chapter gives concluding remarks about the discussion and discussions about the future scope for this work.

2. CHAPTER 2: LITERATURE SURVEY

2.1: VERIFICATION V/S TESTING

2.2: NECESSITY OF TESTING

2.3: HARDWARE SECURITY

2.4: ANTI-COUNTERFEITING TECHNIQUES

2.5:COUNTERFEIT DETECTION TECHNIQUE

2.1. VERIFICATION V/S TESTING:

Process of Testing and Verification should be done in developing any electronic device. Verification is a prefabricated analysis to ensure that the synthesized circuit will give the desired input output functions or not. Testing is a process that will occur after fabrication to check whether there are any manufacturing faults and to validate the chip based on the responses of the chip for a given input function. Below table 2.1 describes the exact differences between the verification and testing.

Table 2.1: differences between the verification and testing

Verification	Testing
❖ Verification is an off chip process	❖ Testing is on chip process
❖ Generally verification can be done at the gate level and RTL level	❖ Testing will be performed after the fabrication of the device
❖ Verification process ensures that the design matches the intended specifications or not	❖ Manufacturing tests, checks whether all the parts of the circuit fabricated correctly or not.
❖ Verification will be done on the circuit only once	❖ Testing will be done on each and every device that is manufactured
❖ It gives the quality of the design	❖ Testing will give the quality of the chip

2.2. NECESSITY OF TESTING:

Since the technology is increasing rapidly, the size of the chip decreases and no of

devices integrated per area increases. So visually we can't inspect the defects that are present in the chip. To verify those defects we have to depend on different tests which are nothing but statistical and functional tests. Any electronic circuit will fail due to the following reasons 1) maybe the design is wrong. 2) Due to low quality test procedure. 3) Because of poor manufacturing process. Testing will detect the failures if it happens because of above three reasons.

Probability of occurrence of defect directly relates to the size of the chip. As the size decreases its value increases. But the IC quality is decided by the test performance, which will give the covering of different types of physical defects [2].

Another important thing about VLSI testing is testing cost. Testing cost varies greatly with respect to the number of pins, time to require for testing a single IC. This cost also depends on the position of particular testing IC. For example, if the IC is tested alone or it is tested on the PCB or it is tested on the system or it is tested on operational system. The cost of testing the IC at these levels will increase 10 folds as it goes from the device to the operational system. The following fig explains the cost pyramid that is the size of the particular level represents cost required to test the IC at a particular level.

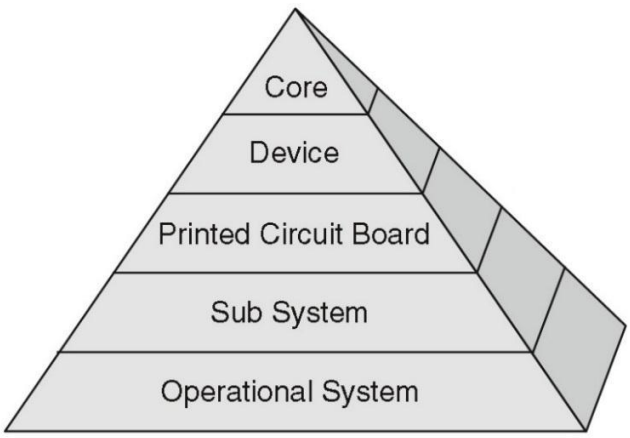


Fig2.1: Testing cost Pyramid [3]

Above fig shows that the cost required to test the IC at the operational system level is approximately 10000 times greater than the cost required at core level.

2.3. HARDWARE SECURITY:

In present days globalization of semiconductor chain is increased to reduce the manufacturing cost of the semiconductor devices. This lead to many security issues [17] like over production of chips, shipping of faulty or partially tested chips, introducing hardware Trojans into the circuit, IC counterfeiting, cloning. Because many cryptographic algorithms are vulnerable to different attacks like side channel attacks, power analysis and differential power analysis. So it became easy to pirate the Intellectual property (IP). Hardware Trojans may insert inside the design house or at the manufacturing centre. Over production of chips or shipping of faulty chips may occur because of the un-trusted foundry and packaging centre. These counterfeiting of ICs lead to some serious problems [32] in some mission critical applications.

Some of the hardware security issues are

2.3.1. Side channel attacks:

Side channel attacks leaks the physical information of the system through physical commodity when an application is executed on that system. For example, it leaks the secret keys of some cryptographic algorithms like RSA and AES. The information of about keys can be leaked from ICs through power analysis, timing analysis, electromagnetic emanations, photonic emissions, scan chains and through faults injected into the circuit.

2.3.2. Hardware Trojans:

A Hardware Trojan is a malicious circuit that attackers add to the original circuit. This Trojan can control, modify and monitor the contents and communication of the original circuit. There are mainly two hardware Trojan scenarios. First: the attacker in the foundry may insert Trojan

into the design. Second: A malicious IP is designed by a person in the third party IP design house or by a person in the in-house design team. Detection of these Trojans became very difficult because of 1). Conventional parametric IC testing methods have limited effectiveness. 2) Because of the technology scaling the limits on the mask and device physics results in nondeterministic behavior in the IC characteristics which makes the distinction between the process variation and Trojan difficult.

2.3.3. IP piracy and IC overbuilding:

Designing cost of IP core is high, so generally while fabricating the ICs the manufacturer can steal the IP core and he may claim the ownership of the IP. In addition to that, while manufacturing the ICs foundry may fabricate more no of ICs then ordered to be delivered. These over produced ICs will enter into market with less cost which will cause huge financial loss to the IP designer. Mainly there are two situations where an IC can pirate one: an attacker in the design house can pirate the IP, second: an attacker in the third party IP core (3PIP) can pirate the IP core.

2.3.4. Reverse Engineering:

Reverse engineering is used to study the internal design of the circuit without the permission from designer. It mainly consists of i) knowing the device's technology used ii) Extracting the gate-level net list iii) Reflecting the functionality of the circuit. This Reverse engineering causes the stealing of IP core. The main aim of the attacker is he has to know the whole design to a desired abstraction level. For this he generally he will use known input-output pairs to check the functional correctness of the circuit. Another problem from the reverse engineering is insertion of hardware Trojans. If an attacker wants to insert Trojans, he has to reverse engineer up to gate-level or RT level.

2.3.5. IC Counterfeiting:

Counterfeit electronic devices are the one whose performance of the material or characteristics of the circuit are misprinted by the vendors intentionally. This counterfeiting became a major problem in the present semiconductor industry. This counterfeits can reduce the performance of the systems like clock frequency instability, life time of device decreases, less memory storage compared to the original device or the whole system may damage. In some mission critical applications, it can cause serious problems. According to the survey conducted by the Alliance group of Gray Market and Counterfeits Abatement 10 percent of these electronic devices which are in the market are counterfeit devices. This represents approximately about 100 billion dollar loss for the original IP vendors for every year. It became very difficult to detect these counterfeit because of their increased sophistication methodologies. Main semiconductor devices which are counterfeited are Analog ICs, Microprocessor IC, Memory IC, Programmable logic IC, Transistors. According to the statistics of ERAI the 5 top most electronic devices counterfeited [34] in 2011 is shown in given below table 2.2

Table 2.2: Top 5 most counterfeited semiconductor devices

Rank	Component type	% of reported incidents
1	Analog IC	25.2%
2	Microprocessor IC	13.4%
3	Memory IC	13.1%
4	Programmable logic IC	8.3%
5	Transistor	7.6%

2.4. ANTI-COUNTERFEITING TECHNIQUES :

As we know counterfeits are illegal and unauthorized components from the original component manufacturer (OCM), and those have less performance with respect to lifetime, speed etc. So we have to detect and avoid those counterfeit devices to enter into the market. Counterfeiting mainly involves recycling and remarking. Almost 80% of the counterfeit devices are from these two categories. Another type of counterfeits are cloning, overbuilding ICs, shifting defective or out of spec ICs.

Taxonomy of counterfeits:

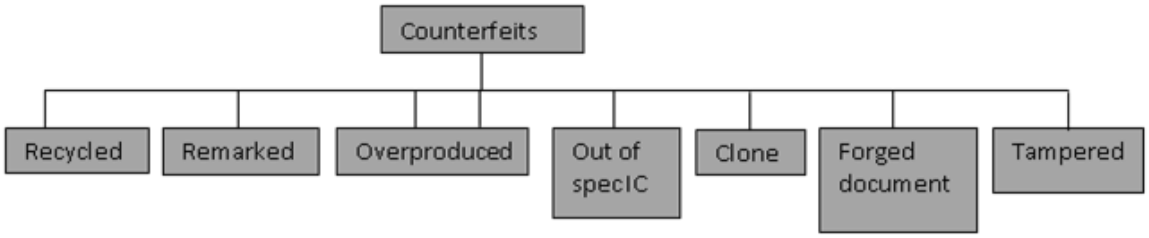


Fig 2.2: taxonomy of counterfeits[34]

Fig above represents the taxonomy of counterfeits. Recycling of components means these are taken from used printed circuit boards (PCB) and after cleaning process these are repackaged and remarked. Overproduced and out of spec ICs enter into the market because of un trusted foundry. Cloning includes reverse engineering, which will retreat the original IP of the design so that they can manufacture duplicate devices which will drastically reduce the high IP designing cost.

Anti-Counterfeiting Techniques:

2.4.1. Using ECID:

This method is mainly used to check the warranty of the devices. In this method each IC is given a particular ID and all these IDs are stored in the database of the IP vendor, so counterfeit

electronics can be detected when its ID is checked against the database. These IDs may be simple like bar codes so by using RF technology these can be scanned.

2.4.2. Hardware Watermarking:

Hardware watermarking has become prominent in present days to prevent the intellectual property in VLSI chips. Hardware watermarking provides a single identification mark for IP by creating a single fingerprint in it. The main aim of watermarking is to design a physical design pattern which can't be duplicated. This can be used as authentication proof. This watermarking can be designed by placing watermarks into the IP core by injecting watermarks into the output combinational logic blocks.

2.4.3. Hardware Metering:

Hardware metering is a technique used to avoid the overproduction of chips by the foundry. It includes different methods, processes and protocols to achieve the control to the IP vender over no of chips fabricated by the foundry. In this method a unique ID is allotted to each chip which is used to unlock the ICs functionality. So if more no of ICs are produced by the foundry than he has to request the vendor for more no of keys. With this we can limit the no of ICs fabricated by the foundry.

Based on the type of authentication provided by the vendor there are mainly two types of hardware metering techniques. 1) Active hardware metering 2) passive hardware metering.

As the above fig represents hardware metering can broadly classify into two types 1*) passive metering 2) Active metering.* Each metering technique is sub classified into non-functional and functional identification methods.

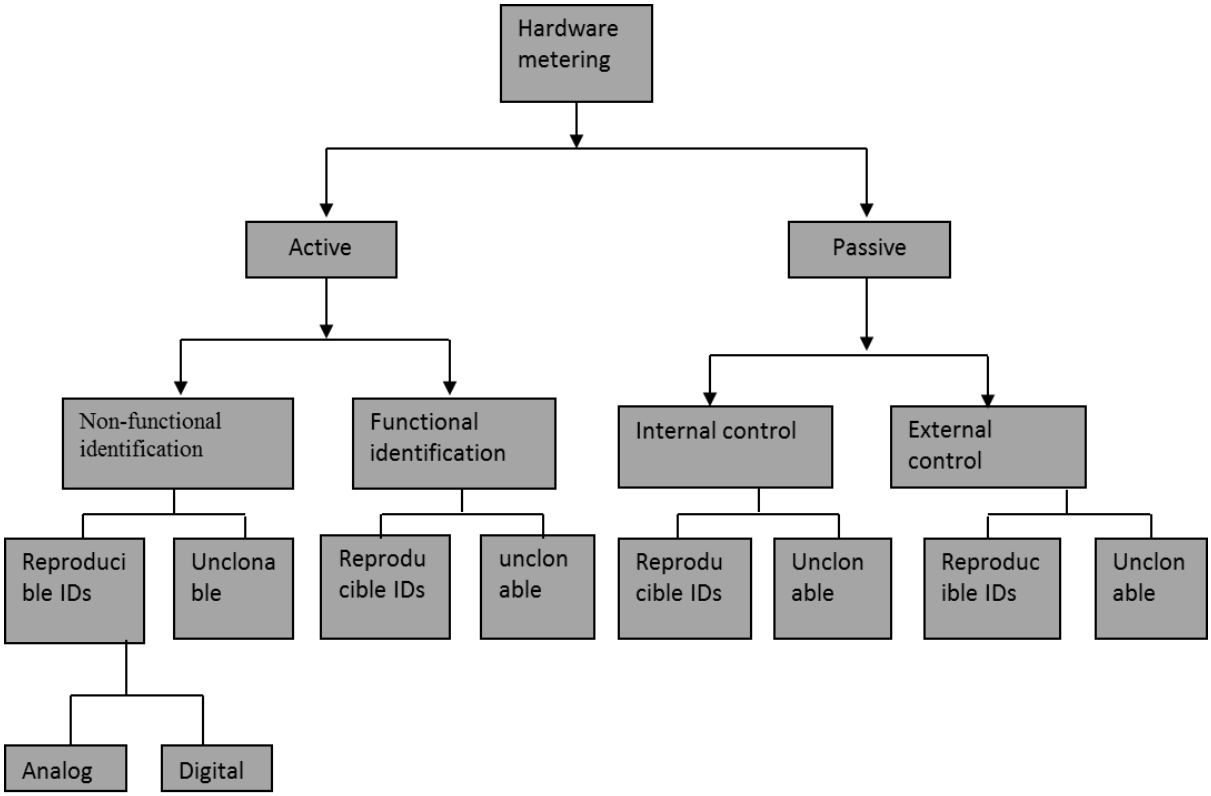


Fig 2.3: Taxonomy of hardware metering [33]

Passive metering:

In Passive metering technique we will assign a unique ID to each chip. This method is used for a long time. This method can be used in two ways, one is by placing a serial number on each device physically. This method is called intended serial number. Second is we will store the serial number in a permanent memory. This method is called digitally stored serial number. Since unique IDs are separate from the functionality of the chip these two methods will come under the category of non-functional identification method. As these serial numbers both intended and digital can be copied and used in another chip these are called reproducible. Therefore these methods come under the name of reproducible non-functional identification methods.

But during recent times these reproducible serial numbers are vulnerable to the cloning attacks frequently. So some other techniques have been proposed which are difficult to cloning.

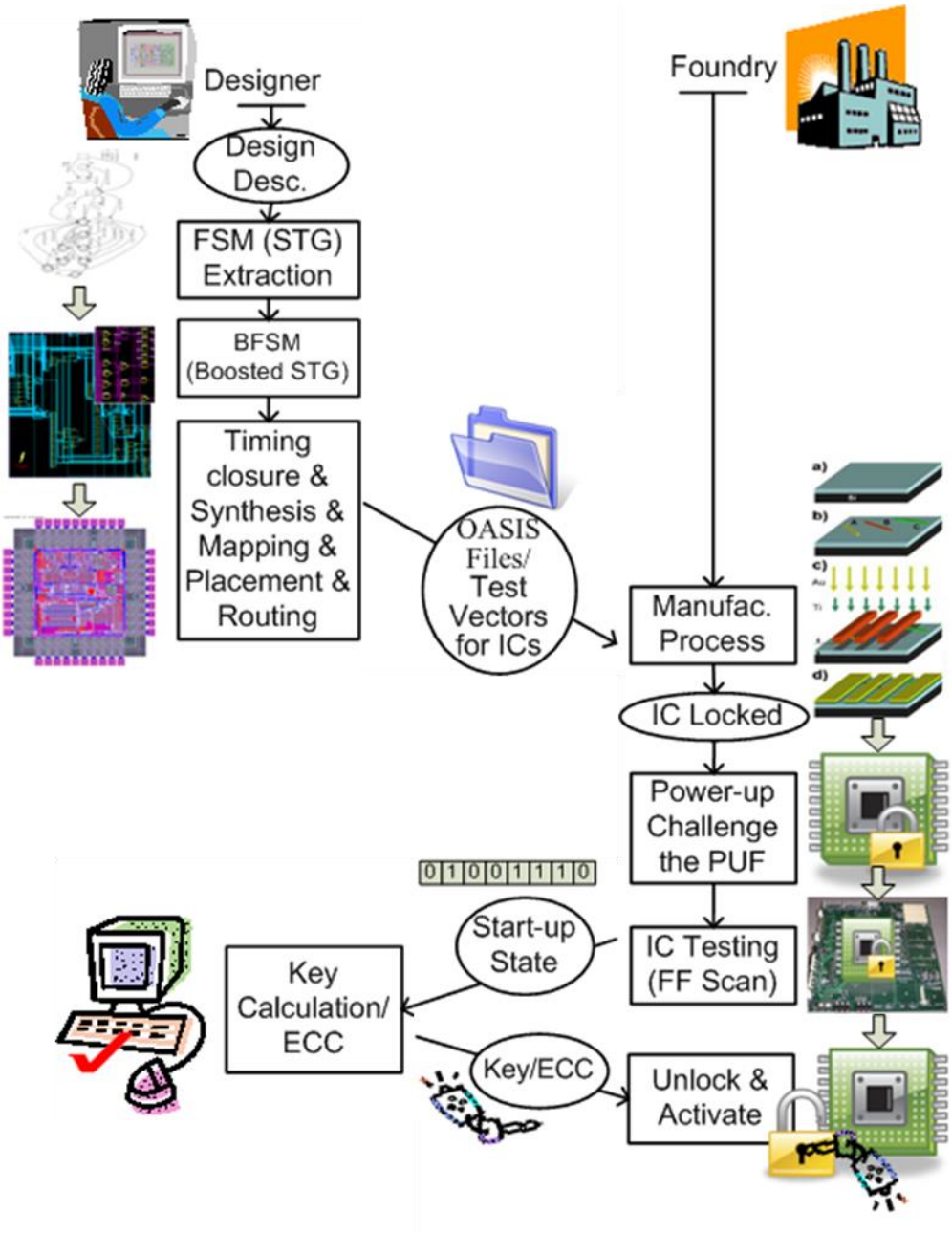
These type of methods uses random process variations to generate the IDs which are unclonable. Since these random process variations can't be controlled or expected, these will not be cloned. These unclonable IDs can be generated using physical unclonable functions (PUFs). So this method comes under the category of unclonble non-functional identification. Slowly improvements in the derivation of these IDs have been proposed. In these methods those serial numbers are attached to the functionality of the chip. So when chip starts functioning, it will generate a signature which is used to identify the chip. This method is called functional identification. In this method both reproducible and unclonable methods can be used to generate the single response format to identify the chip.

Active metering:

Active metering technique provides uniqueness for each chip and in addition to that it can be used control, monitor or disable the chips. This can be achieved using two ways 1) during the power on state IC will be locked. 2) by using FSM chip is unlocked, when the correct key is given then only chip is unlocked otherwise chip will be in locked state.

Active metering techniques can be classified into two categories *1) active external hardware metering 2) active internal hardware metering.* In internal hardware metering states and transitions of FSM are internally integrated to unlock the functionality. But in external hardware metering cryptography methods are used to unlock the IC functionality. This hardware metering method is used to avoid the overbuilding of chips without the permission from IP vendor. When the chips are fabricated then before testing ICs are unlocked by using the secret keys of FSM, after that, foundry will test the IC functionality and tests it whether if fail or pass.

How an IC can be enabled is shown in following fig:



2.4.: IC enabling in active hardware metering [33]

2.4.4. Secure Split Test (SST):

In previous methods that are proposed to avoid the counterfeits have following disadvantages

1) Since we are giving the key before testing, the foundry may send the partially passed chips to the open market for lower cost. It will affect the financial status of the original company.
2) The Foundry may request for the additional keys by claiming low yielding of the chips so that they can ship those additional ICs into the market.

These disadvantages can be eliminated by using secure split test (SST). In this method we can control the counterfeits by giving post production testing control of the IP vendor. Here output signatures are scrambled so that the actual responses can't be expected without the prior knowledge of particular sequences of bits. So the only IP owner can decide whether the chip pass or fail. After that only for passed chips, IP owner can send the actual key to unlock the chip. So failed chips can't be unlocked and overproduced chips also can't be locked, this eliminates the problem of counterfeits.

2.5. COUNTERFEIT DETECTION TECHNIQUES:

Since the attention on counterfeits is increasesing research on detection of these counterfeits is also drastically increases. Based on the type of inspections, those are broadly classified into three categories 1) *physical inspections 2) Electrical inspections 3) Aging-Based fingerprints*

All these techniques are used to detect different types of counterfeits that are arising in the recent days.

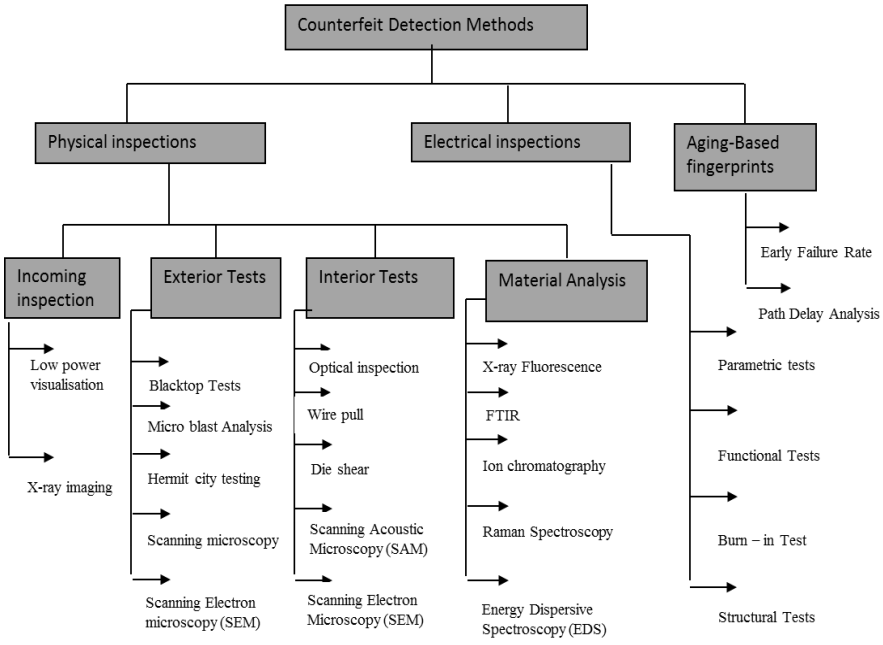


Fig 2.5: Taxonomy of counterfeit detection methods [34]

In this thesis, we are concentrating on the anti-counterfeiting techniques especially on Secure Split Test (SST) and we had done work on improving the security of the IP design from counterfeit electronics.

3. CHAPTER 3: TOOLS USED

3.1: DESIGN FOR TESTABILITY (DFT^{TM})

3.2: TETRAMAX^{TM}

3.1. DESIGN FOR TESTABILITY (DFT):

Since the technology is advancing, the size of the chip gets decreases and probability of occurrence of defect increases. The quality of a particular foundry depends on the Yield of the chips. Yield is nothing but the ratio of no of non-defective ICs produced to the total no of ICs fabricated. To get more yields the foundry has to fabricate more no of non-defective ICs and finally we have to isolate defective ICs from non-defective ones. This non-defective should be shipped into the market. To separate those ICs we need to have some simple test plans and excellent test pattern generation schemes. Testing procedure, required to get more test coverage over different manufacturing defects is called Design For Testability (DFT).

Usually these DFT methods are two types [2] 1) Ad-hoc method 2) Structured method.

Ad-hoc method:

These methods mainly depend on good design tactics learnt from the experience. But this method contains very less controllability and observability of different points. Mainly,on this ad-hoc technique it is very difficult human inspection as the size of circuit is large and even some times experts may not find the position of the defects. One more thing is these DFT methods will not ensure good fault coverage when test patterns are generated by Automatic Test Pattern Generators (ATPG). So to overcome these disadvantages Structured DFT is proposed.

Structured DFT:

Structured DFT performs testing by adding extra logic circuits to the original circuit such that the original functionality of the circuit remains unchanged. In this method circuit generally operates in more than one mode (i.e. functional mode and testing mode).Every electronic

design comprises of mainly 3 types of components 1) Digital logic circuits 2) Memory blocks 3) Analog or mixed signal circuits. There are different DFT methodologies available for each type component [6]. Most frequently used Structured DFT techniques for Digital circuits are 1) scan design method 1) Built-In self-test.

Scan design method:

Idea behind using this scan design is to achieve controllability and observability mainly for flip-flops. For the past few years this method has become prominent methodology for digital circuit testing. Following fig represents the architecture of scan testing. There are four scan structures for the testing of digital circuits 1) multiplexed flip-flop 2) clocked scan 3) level sensitive scan design (LSSD) 4) Auxiliary clock LSSD. Here throughout discussion, we will use multiplexed flip flop style structure.

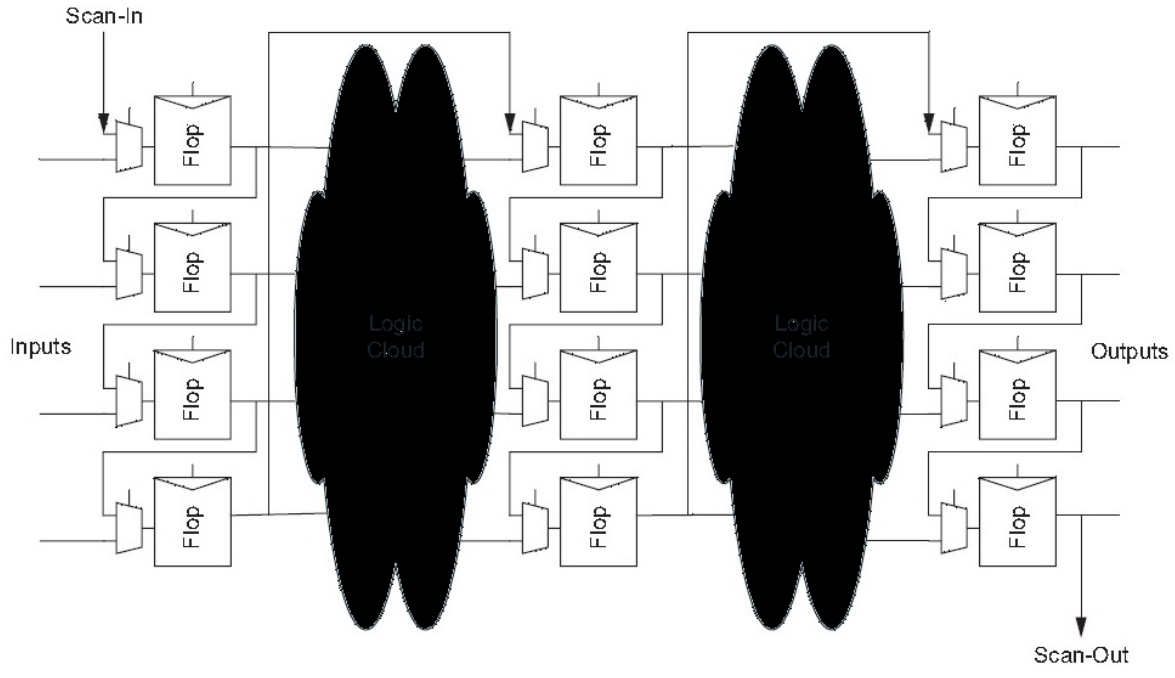
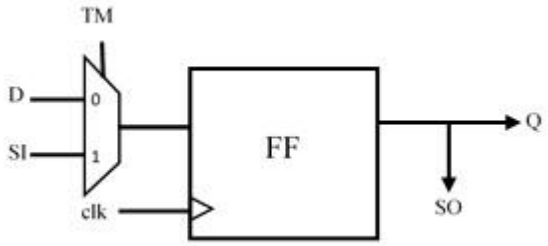


Fig 3.1: architecture for DFT testing [6]

In this method circuit will operate in two modes 1) normal mode 2) test mode. In

multiplexed flip-flop method every flip-flop in the design is replaced with scanned flip-flop which is nothing but addition of multiplexer before the flip-flop to change the mode of operation. This multiplexer has two inputs, one is actual flip-flop input and second is scan input. Control signal for the multiplexer is scan enable signal. When this signal enabled circuit will operate in test mode, otherwise it will be in normal mode. In test mode all the flip-flops form a single chain and acts like shift register. It should have at least one PI and one PO.



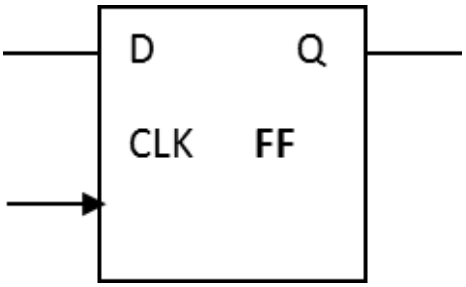


Fig 3.2: scanned flip flopFig 3.3: normal flip flop

Keeping the whole flip-flops in a single scan chain will increase the testing time, which will increase the test cost. So we can group some flip-flops, such that the design contains multiple scan chains and each scan chain will contain separate scan in and scan out pins with same scan enable pin.

If we increase the no of scan chains reduces the test time but pins (scan channels) required to test the IC on ATE increases and memory required to store those results also increases. No of channels and memory space on ATE is limited so if we go for higher scan chains again test cost will increase. For that we have to trade-off between no of channels required and testing time of the circuit.

3.2. TETRAMAX™

3.2.1. Introduction:

Test vectors have to be generated to test the chip after fabrication to find any faults during the manufacturing process. There are different fault models which will occured at the time fabrication. For example Stuck-at faults, Path delay faults, bridging faults, quiescent current (IDDQ) faults, Delay faults, Transition delay faults [2] etc. these are all structural faults. In addition these functional faults also can occur.

To test all these faults and to increase the quality of the test different algorithmic methods has been deployed to generate the test patterns. This process of generating test patterns algorithmically is known as Automatic Test Pattern Generation (ATPG). This test pattern that has been generated should have good test coverage to detect faults in the device which is under test (DUT) and testing time should be as small as possible.

This ATPG can be accomplished by effective algorithms and CAD tool [6]. All these algorithms and tools use some of the design and fault models. Usually, these design models are derived from circuit net list.

In this chapter we will discuss about the basic flow of ATPG using industry standard tools from Synopsys for stuck-at-faults. Some Synopsys tools are Design compiler (DC™), Verilog Compiler Simulator (VCS™), DFTMAX™, Primetime and TetraMAX™. These test patterns are generated for the sequential benchmark circuits (ISCAS'89) like S38417.

3.2.2. FLOW OF ATPG FOR STUCK-AT-FAULTS:

Simple and basic fault model to test the electronic circuit is the Stuck-at-fault-model. Flow of ATPG for stuck-at-fault (S-A) model [6] can be shown in fig.

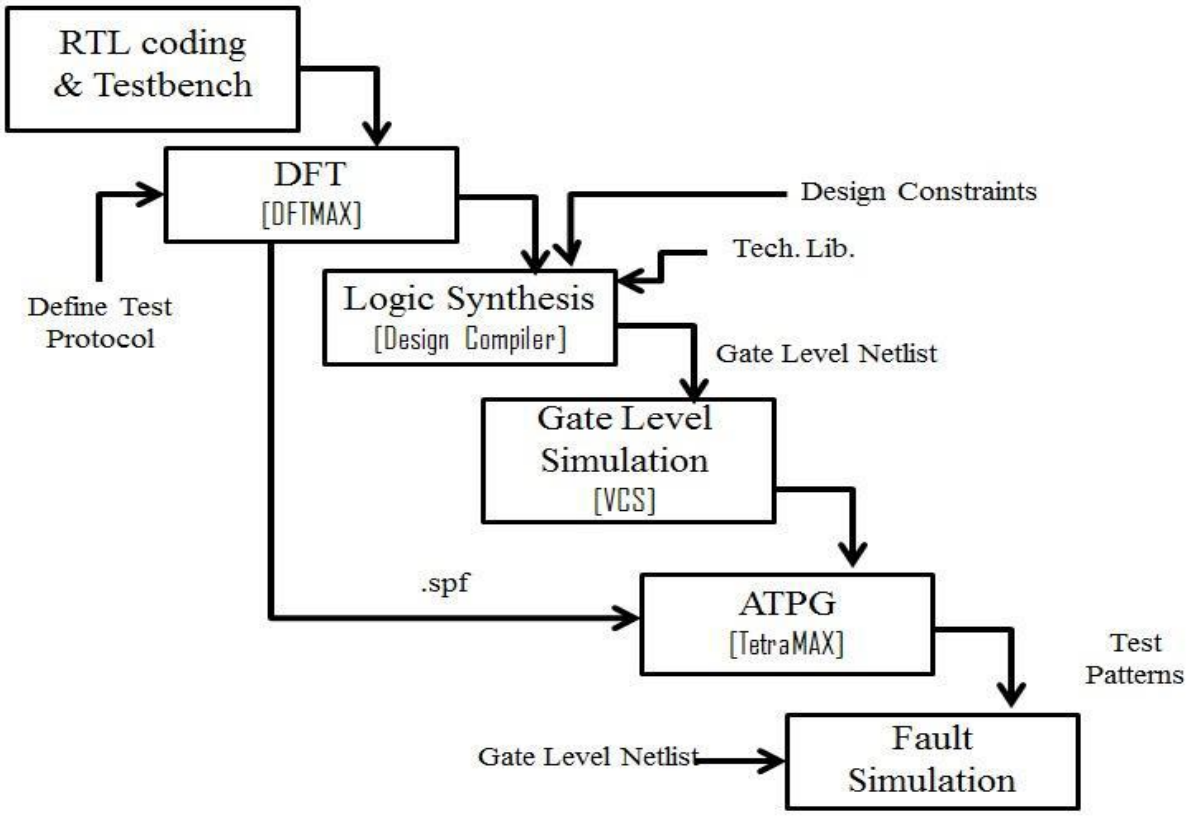


Fig 3.4: Test generation flow for stuck-at fault with Synopsys tools [6]

Any digital circuit that is designed, its functionality should be verified with proper test pattern. The design may be at Register Transfer Level and in either VHDL or Verilog format. Here for experimenting we are taking benchmark circuit S38417 in Verilog format and CMOS 65nm library by TSMC ltd. is used to synthesis the design.

To generate the test patterns first we have to generate the net list file from the DFTMAX^{TM} using one of the best scan methodologies available among four DFT structures. This DFTMAX^{TM} is used to insert the DFT into the design. Here we are using multiplexed scan style throughout our experiment. Test protocol gives the list of signals and their job that are using in the

design. Test signals may be scan in, scan out, scan clock etc... After creating test protocol design rules are checked and if any violations are there those will be fixed before creating the .spf (STILL Procedure File). In addition to these no of scan chains that we are using is also specified.

After that design is fed with any optimization constraints like speed, power and area. Synthesis tool will try to optimize the design in the same order of precedence. Design compiler (DC^{TM}) also tries to optimize the constraints that are implicitly defined by technology library. Now the synthesized tool will give the net list file for a given test protocol, library and constraints. This DFT structure is added only to sequential circuits, combinational circuits will not require any DFT structure to generate the test patterns because combinational circuit faults can be detected easily from their PIs and POs.

Gate level net list and STILL Procedure File that are generated in DFTMAX^{TM} are given to TetraMAX^{TM}, which is an ATPG tool to generate the test patterns for detecting the Stuck-at-faults. This tool will try to reduce the set of test patterns required to detect the faults. These test patterns can be written in different forms like WGL, Verilog, VHDL, STIL formats. We will use Verilog single file format to write the test patterns and these patterns are simulated with gate level net list that is generated using DFTMAX^{TM} and DC^{TM}.

4. CHAPTER 4: ANTI-COUNTERFIET TECHINQUES

4.1: INTRODUCTION

4.2: SECURE SPLIT TEST (SST)

4.3: CONNECTICUT SECURE SPLIT TEST (CSST)

4.1. INTRODUCTION:

In present days as the technology is increasing many fabless IP designing companies can't bear the cost of sophisticated equipment. So all the fabless companies outsourcing their IP designs for fabricating the devices to reduce the manufacturing cost. Although testing cost is recurring cost, every chip gets fabricated must be tested. Generally after testing each device only passed chips should send into the market and all the failed chips and partially passed chips should be discarded. But Assemble Packaging and Test (APT) centres will sell these unfit ICs also to the customers for low cost. Since the IP designing cost is high many foundries and test centres can produce more no of ICs without the permission from IP owner. These two problems became the major threat to the present semiconductor industry. This is called counterfeiting and devices are called counterfeit electronics.To overcome these counterfeits many approaches are proposed by the researchers. Among them Hardware metering is one technique which will avoid the production of extra chips then they are ordered. But it can't control the flow of faulty chips into the market. To solve these two problems Secure Split Test (SST) is proposed by *Gustavo k. Contreras, Md. Tauhidur Rahman and Mohammad Tehranipoor*, which will control all types of counterfeits.

4.2. SECURE SPLIT TEST (SST):

Generally, testing of IC is done at test centers and validity of that IC also decided by the test centers. And IC is unlocked before the testing of the IC. But this method called Secure Split Test (SST) prevents the counterfeiting by unlocking the IC after testing and ICs are unlocked by the IP owner only after they are passed. Normally IP owner will not involve in testing once the design is completed but SST provides IP owner involvement without his physical presence and control over the decision of pass or fail of IC. This can be achieved by adding two additional logic blocks in the design.

The two blocks are 1) Functional locking block, which will make sure that only unlocked ICs will give the correct functionality. 2) Scan locking block, this block secures the functional results so that no one other than the IP owner can't modify or attack the SST structure.

Functional Locking Block:

Fig 4.1: shows the schematic of functional locking block

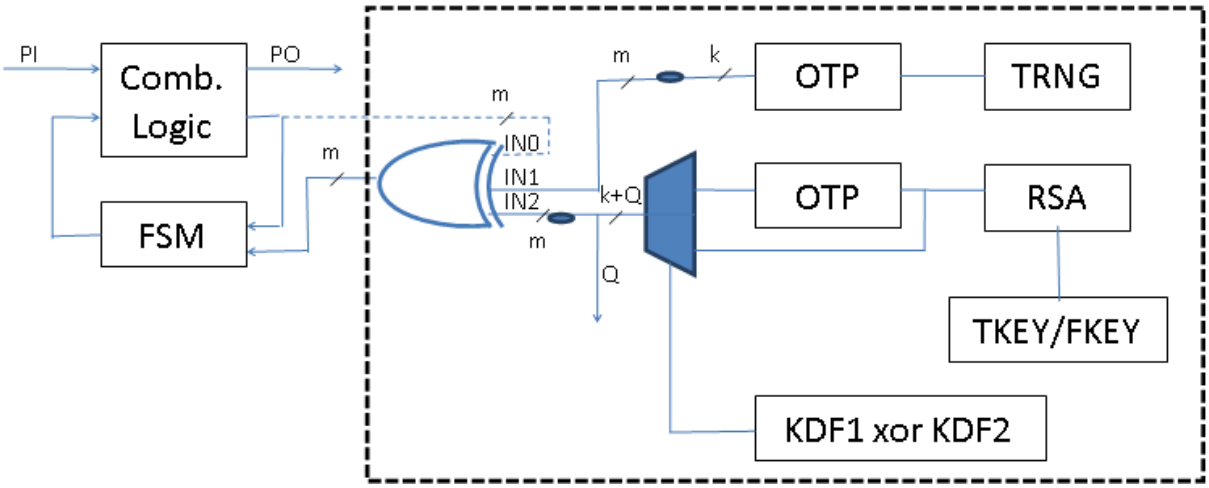


Fig 4.1: functional locking block [12]

Functional locking mainly contains 1) True Random Number Generator 2) RSA Decryption block 3) XOR_F mask.

XOR mask:

XOR_F mask is combination of m 3-input XOR gates. It is into the design. Among those three inputs IN0 is from the original inputs. When the inputs from IN1 and IN2 are same then the XOR gate of that particular bit will act as buffer otherwise it will act like inverter. IN1 is from the output of TRNG which is stored in One Time Programmable (OTP). IN2 is from the output of RSA Decryption block. When the correct key is applied then only IN2 is same as IN1 then all the XORs will act as buffers and it will give correct functionality otherwise some of the bits are reversed.**True**

Random Number Generator:

Random Number Generators are the one which will generate the numbers randomly that can't be even predicted. Here that TRNG is stored in a one-time programmable (OTP) memory.

RSA:

RSA is one of the standard cryptographic methods that are used in present days. It is derived by Ron Rivest, Adi Shamir, and Leonald Adleman. Based on TKEY or FKEY given to the RSA this decryption block decrypt the given input that is given to another OTP which acts as input to the IN2 to the XOR_F mask.

Scan Locking Block:

Scan locking block make sure that unknown users can't read or modify the functional results of the design. Following fig shows the block diagram of scan locking block.Design is first inserted with DFT. Scan chain inputs are make transparent or inverting by using XOR gates. This decision of making inverting is decided by TKEY and FKEY. Similarly outputs are also fed with XOR gates. The outcome of the results can't be scanned by the test centres because which XORs are inverted is known to only IP owner.

Communication flow between IP owner and Foundry:

When the device is put under test then TRN is generated. That TRN is sent to the IP owner; IP owner will modify the actual TRN and add some additional bits which will control the inputs to the XOR gates of scan locking block. This TRN mod is encrypted using the private key of IP owner to generate the TKEY. This key is sent to the testing centre which is used to decrypt the

RSA block, output of the RSA is some inverted bits of the original TRN. So some bits of the scan results are inverted but only IP owner knows which bits are inverted. Testing results are sent to the owner, he will decide whether IC fail or pass. After passing the test then only IP owner release the original FKEY to the testing centre.

Main disadvantages of SST are

1) Communication flow between the IP owner and foundry is complex, since two times communication is required.
2) Less security since only XORs are used which can be attacked easily.

These disadvantages are overcome by improving the hardware which is proposed by the same researchers. This method is called Connecticut Secure Split Test (CSST).

4.3. CONNECTICUT SECURE SPLIT TEST (CSST):

CSST improves communication flow by modifying the functional block, this method talks about the whole wafer [13] [14]. Here all the ICs in the wafer are tested then TRN is generated for each IC that is sent to the IP owner. Each TRN is encrypted and cipher text is forward to the foundry. Using these encrypted TRNs foundry collects the output signatures and those will sent to the IP owner along with encrypted TRN. Then IP owner decides fail or pass of IC, therefore here only one time communication is sufficient here. Modified functional locking block and scan locking block are shown in fig 4.2.

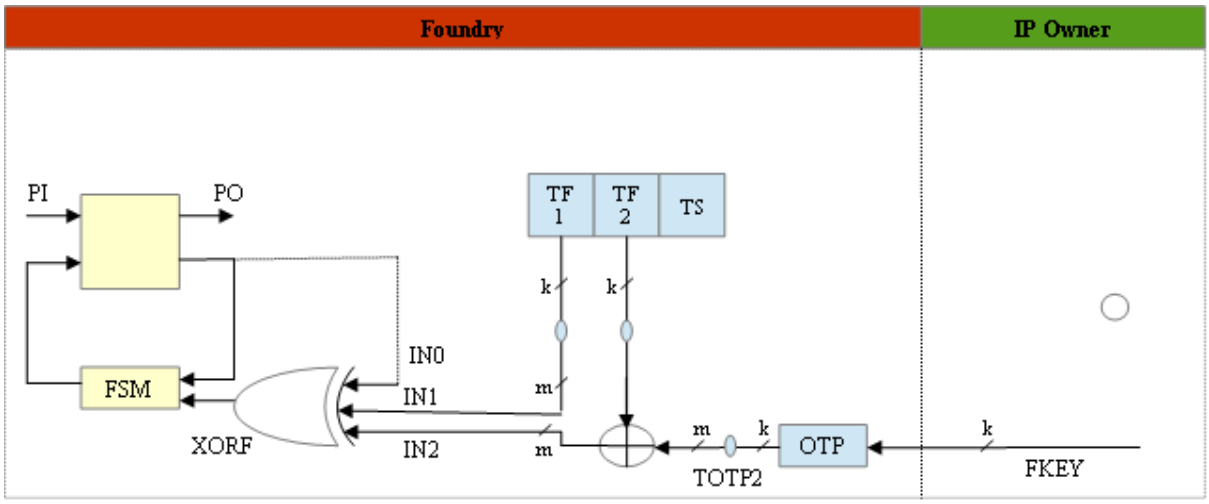


Fig 4.2: block diagram of functional locking block [13] [14]

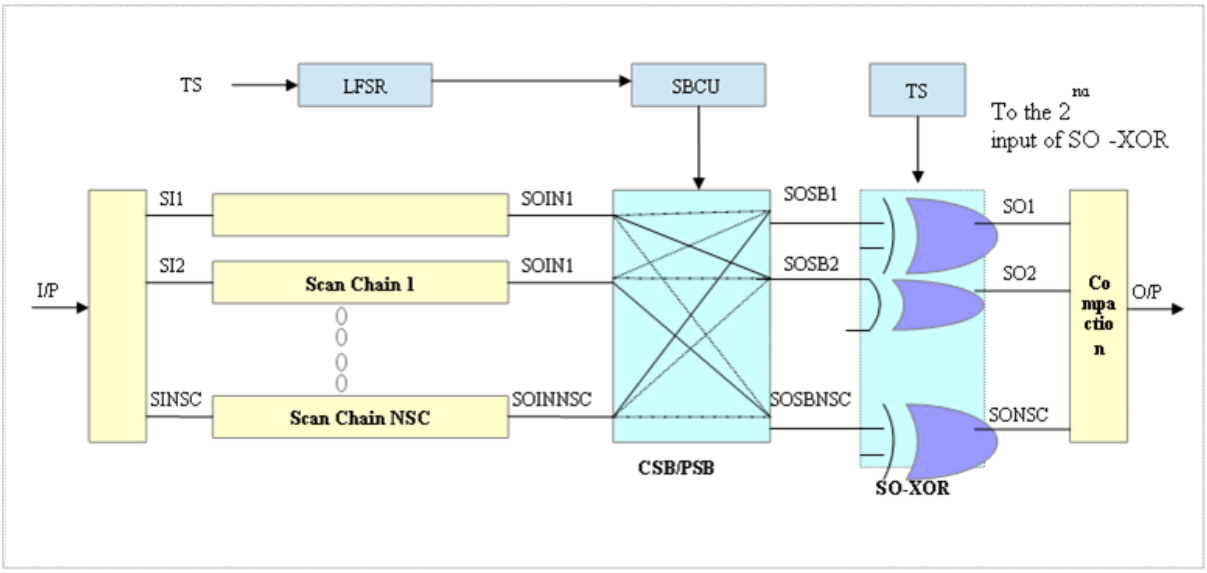


Fig 4.3: block diagram of scan locking block [13] [14]

Security of the design is improved by adding scrambler block to the outputs of the scan chains. That scrambling is controlled by LFSR and scrambling block control unit.

5. CHAPTER 5: PUF BASED SST

5.1: INTRODUCTION

5.2 PUF BASED SST (PUF-SST):

5.3: SCRAMBLER BLOCK

5.4: RESULTS AND DISCUSSION

5.1. INTRODUCTION:

The common security problems known in semiconductor industry are counterfeit chips, IP protection, hardware Trojans, side channel analysis of cryptographic engines, and debug security against reverse engineering schemes. Hardware metering is one promising technique to check the overproduction of chips in untrusted foundries. Active hardware metering using physical unclonable functions (PUF) is an attractive solution to counter over production of chips.The secure split test (SST) technique was proposed in [12] to mitigate the infiltration of failed or out of specification chips into supply chain from APT centres. An improvement or simplified approach for SST called Connecticut SST (CSST) was proposed by same researchers in [14] [13].

This work is an improvement to the CSST proposed in [13]. In CSST, chips are tested for manufacturing faults and functional key for good chips is generated and programmed into the one time programmable memory (OTP). In recent times, there is a need to incorporate functional tests in production testing of integrated circuits. The modern day System on chip testing demands inclusion of few critical functional tests during final production test [29, 30]. CSST architecture support structural tests and does not address functional testing. In this work, we propose a novel SST architecture which includes both structural and functional tests during final production test called PUF based Secure Split Test (PUT-SST).

5.2. PHYSICAL UNCLONABLE FUNCTION BASED SECURE SPLIT TEST (PUF-SST):

The figure 4 shows the block diagram of the proposed architecture. PUF-SST Architecture comprises of Arbiter based PUF, Error Correcting Code (ECC) block for PUF responses, RSA blocks for PUF enrolment, Scrambler, Pseudo Random Number Generator (PRNG) for PUF challenge generation and flipping circuit for inverting some bits of Random Number.

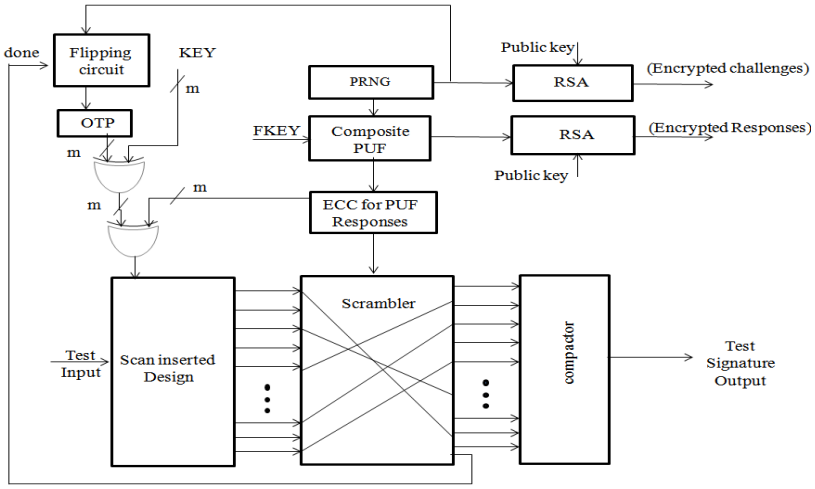


Fig 5.1: Block diagram of PUF-SST

Operation of the PUF based SST:

5.2.1. PRNG:

Random Number Generators are the circuits which will generate the numbers randomly without any prediction. These Random Number Generators can classified into two types 1) Pseudo Random Number Generators (PRNG), 2) True Random Number Generator (TRNG).

PRNG: These use a formula to generate numbers which behave very like genuine random numbers and are widely used for simulations of random processes and statistical methods. These random numbers are generated by using some predefined formulas with a seed to start the number generation.

TRNG: A hardware (true) random number generator is a piece of electronics that plugs into a computer and produces genuine random numbers as opposed to the *pseudo-random* numbers. Generally these are generated with natural phenomena like noise, voltage, and some gate delays Presently I have designed the random number by using the ring oscillator circuits by varying the delays of invertors.

Fig 5.2 shows the simulated waveform for generating the Random number

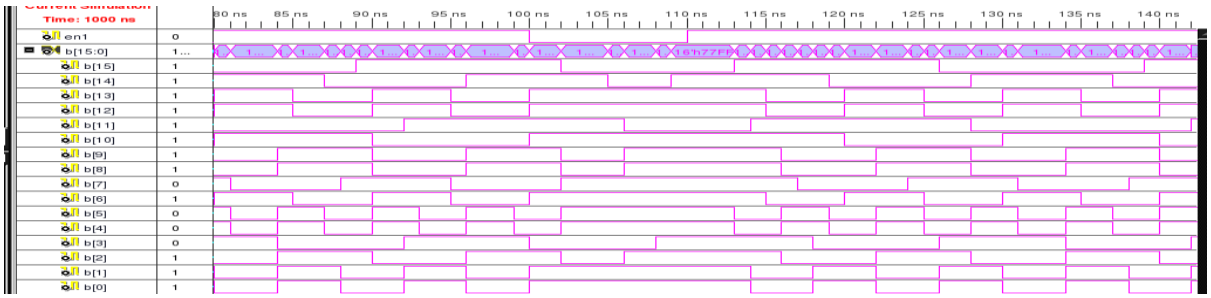


Fig 5.2: true random number generator wave form

In this work first PRNG is used to generate the numbers which will acts like stimulus to the Arbiter PUF for required no of clocks. For each clock cycle one challenge response pair (CRP) is generated from the PUF and those are stored in the database. After taking required no of CRPs test patterns for scan test are applied to the device under test (DUT), these responses are scrambled using scramble block. These responses are sent to the compactor circuit which will give signature output. Control to the scrambler logic block to scrambler the scan outputs comes from the PUF circuit. After getting the required CRPs next PUF output will acts as the control to the scrambler block.

Signatures from the output of the compactor circuit and Electronic Chip ID (ECID) are sent to the design house or Original Chip Manufacturer (OCM). All the CRPs coming from the PUF are encrypted using RSA public key of the design house. This encrypted responses are Decrypted by the design house using private key. So design house can find the control input bits to the scrambler and that will decide the PASS/FAIL of the chip by comparing with the signatures obtained from foundry.

5.2.2. RSA BLOCK:

Cryptography:

Cryptographic methods can be classified into two types based on the sharing of secret key.

1) Symmetric key cryptography 2) Non-symmetric key cryptography.

Symmetric key cryptography:

In Symmetric key cryptographic methods both sending and receiving parties have the same secret key for Encryption and Decryption of the message. In this method messages can be transferred in the form of blocks or streams.

Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are the symmetric kind of Cryptographic methods.

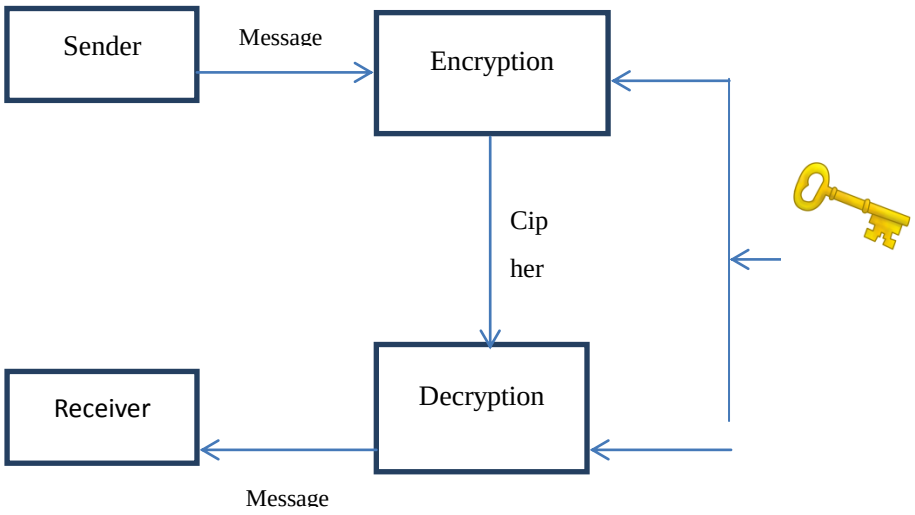


Fig 5.3: AES cryptography block diagram

Non-Symmetric key cryptography:

Symmetric key cryptographic methods will have the same key for Encryption and Decryption. Here key management is needed to precede secure cryptography. So Non-cryptographic method has been proposed which will have two separate keys for both Encryption and Decryption.

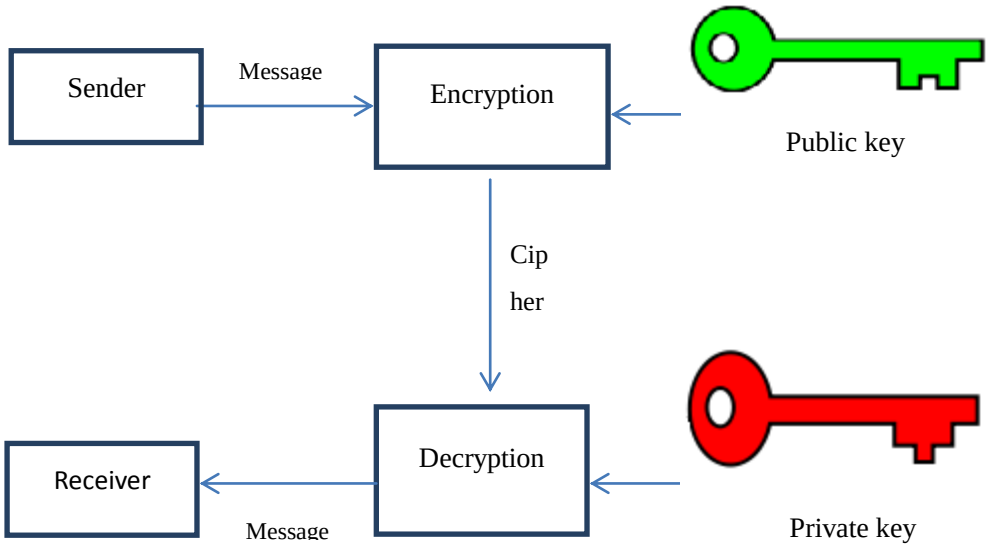


Fig 5.4: RSA Cryptography block diagram

RSA is one of the first practicable public key crypto systems and is widely used for secure data transmission. It stands for R: Ron Rivest, S: Adi Shamir, A: Leonard Adleman

The RSA algorithm involves three steps:

1) Key generation
2) Encryption
3) Decryption

Key generation:

RSA involves a public key and a private key.. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

The keys for the RSA algorithm are generated the following way

1) Choose two distinct prime numbers p,q
2) Compute p*q

3) Compute o(n) =(p-1)*(q-1)

4) Choose an integer *e* such that 1 < *e* < o(*n*) and gcd(e,o(n)) =1

5) Determine *d* as $d \equiv e^{-1} \pmod{o(n)}$ where d is private key and e is the public key. d is called multiplicative inverse of e.

Here we calculate'd' using Euclidean algorithm [8] [9] [11]

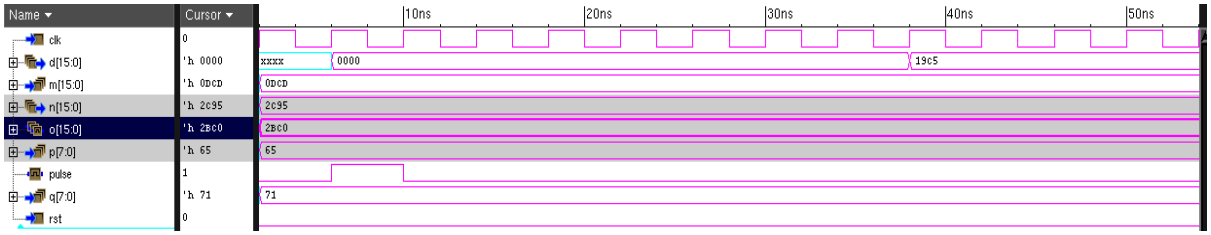


Fig 5.5: RSA key generation

Encryption:

In encryption first we will convert our message into a number then we will encrypt the number using modular multiplication and public key.

Let 'm 'be the my message and (n,e) be the my public key then my cipher text will be

$$c \equiv m^e \pmod{n}$$

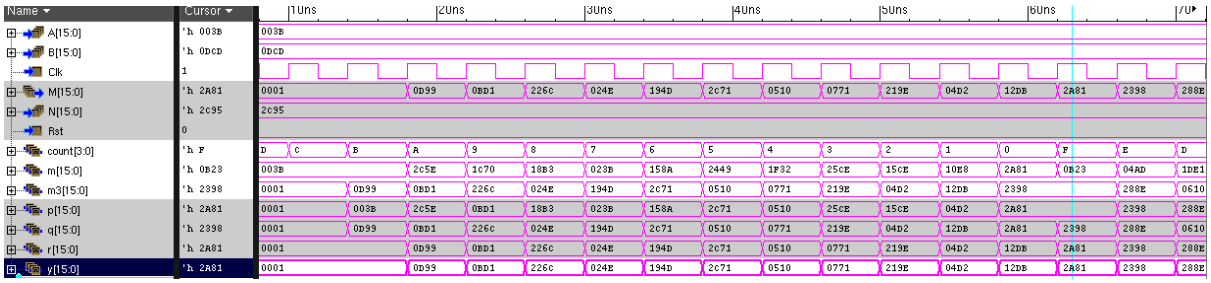


Fig 5.6: RSA encryption wave form

Decryption:

Now at the receiving side receiver can recover the message from C by using the same modular multiplication and private key

$$m \equiv c^d \pmod{n}$$

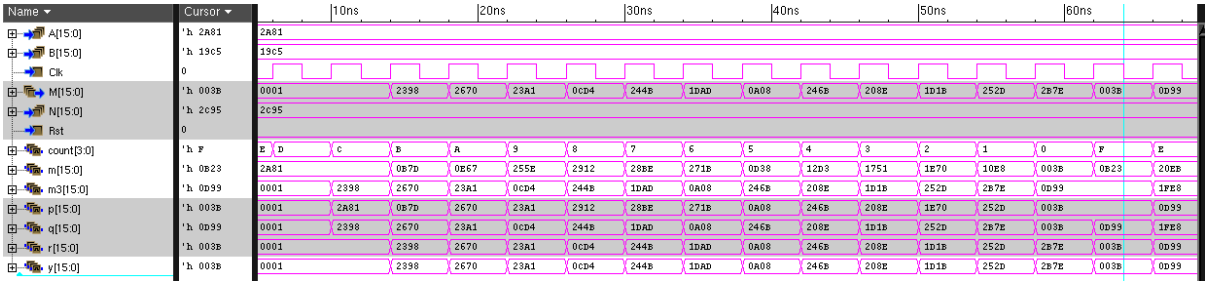


Fig 5.7: Decrypted waveform

All the CRP's of PUF is collected and stored in a server for future device authentication purpose. Among all those CRP's it is easy to find out the challenge (stimulus) to PUF which will generate the functional key to unlock the design. No of CRPs collected is purely depends on the no of chips manufactured by the design house.

For performing the functional test, the functional key which will used to generate the ID from the PUF to unlock the IC is shared with ATP center. By applying this functional key to PUF as input, ATP center will perform functional testing. Initially, all values in the One-Time Programmable (OTP) memory is logic '0'. The XOR gates will act like a NOT gate when one of the inputs is fixed as logic '1' and as a buffer when input is fixed as logic '0'. ATP center will apply FKEY to PUF and KEY (all zeroes of length 'm'). Functional key generated by PUF will unlock the design for functional test through the XOR gate (which acts like a buffer). The same PUF response is used to scramble the test response. After a functional test response is collected and scrambled completely, scrambling block generates the done signal. The signature for scrambled output is generated using compactor.

When the done signal is generated PRNG will generate the random number. This random number will be given to flipping circuit and RSA encryption block. This encrypted PRN, ECIDs and signatures will send to design house to check the functional test. That flipping circuit will invert some bits of the random number. Those bits which are flipped is only known to the design house.

This number will store in OTP. The same number will be given as key to the end user. In this modified SST scan locking block is not modified except the control input to the scrambler.

5.3. SCRAMBLING BLOCK:

The Scrambler is a device that will alter the order of the input string to the order of output string of same no of bits based on the control inputs given to the scrambling block. Sothis scrambling block is used so that scanned outputs can't be read out directly by the unknown persons without knowing the control inputs given to the scrambling block. Following fig shows the block diagram of scrambler having four inputs and four outputs (4x4 scrambler block).Following fig shows the scrambler block.

Below fig represents the block diagram of the scrambler block with four inputs and four outputs which will alter the order of inputs from outputs. By using control bits particular inputs goes to different outputs.

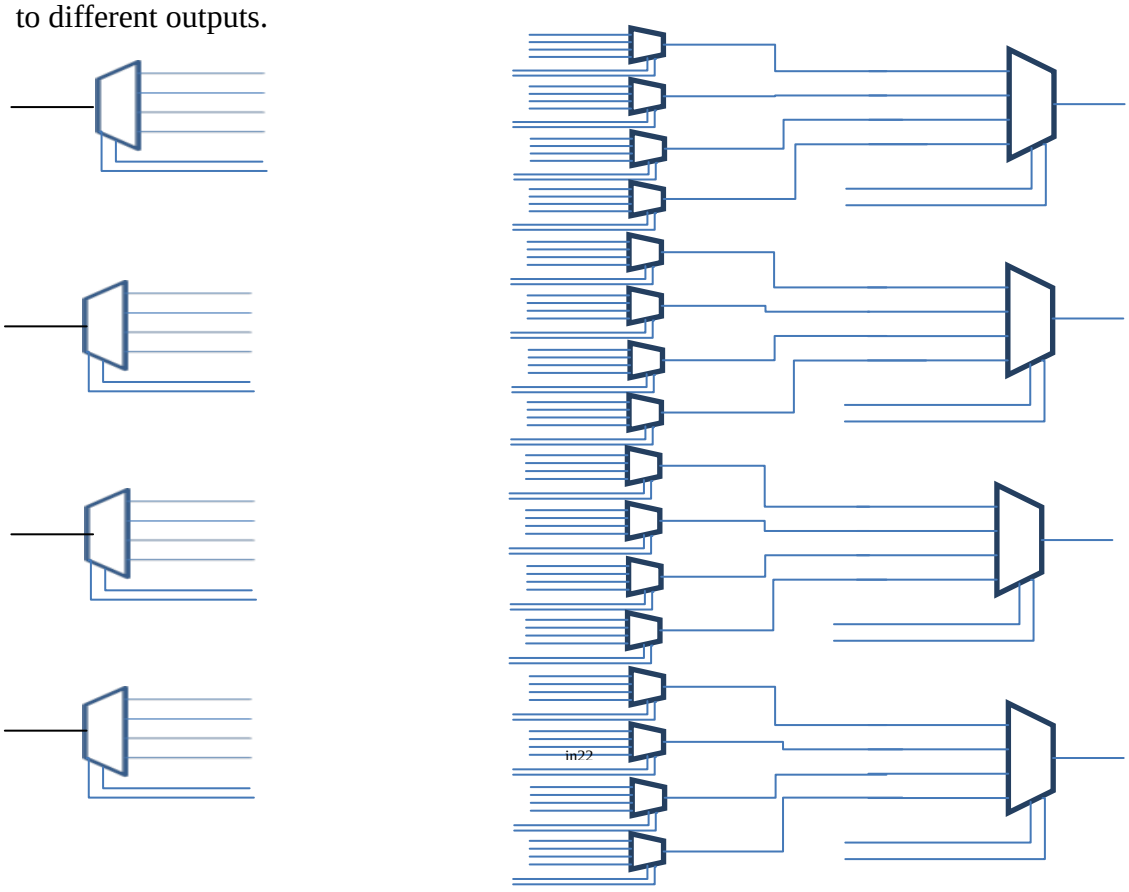


Fig 5.8: block diagram of scrambler block

Communication between design house and foundry:

First encrypted PUF CRPs and ECIDs are sent to the design house by the testing center. Then passed chip ECIDs and their functional key (FKEY) are shared to the test centre by the design house for the functional test. Functional test signatures along with their ECIDs are sent to the design house by the test centre. Finally FKEY and key both are given to the end user by the design house for the passed dies.

Drawbacks of PUF-SST:

1) The proposed SST architecture is complicated structure in comparison with earlier SST architectures. This architecture requires two RSA encryption blocks. The Arbiter PUF is large in area, when compared with TRNG and OTP based SST architecture proposed earlier.
2) Since more no of blocks are used like scrambler, PUF and RSA blocks more area is required.
3) More no of CRPs are taken high memory spacing is required and some extra time is required to collect CRPs.

Advantages of PUF-SST:

1) Since we are not using any memory devices, it is very hard for reverse engineering so design security is high.
2) We can perform functional test with only few extra area overhead.

5.4. RESULTS OF THE PUF-SST:

Hamming Distance analysis:

The hamming distance (HD) is a popular metric to analyze the security strength. The average hamming distance for the scan locking block with 10 scan chains and XOR gates inserted at the outputs of the scan chains is tabulated in the below table. As the no of XOR gates increases hamming distance is also increased, but an average of ~50% is a good range for hamming distance.

Area overhead analysis:

Area overhead means extra area required for the insertion of extra blocks in order achieve high hamming distance. Here presently we are adding only XOR gates at the outputs of the scan chains.Table 5.1 shown below gives the overall analysis about the Hamming distance, power dissipated by the design (Dynamic and leakage), and Area overhead analysis and simulation times for the benchmark circuit S38417 by varying no of XOR gates at the output of scrambler block.Table 5.2 shows the comparison of hamming distance among the PUF-SST, SST and CSST and Table 5.3 shows the Hamming distance analysis for various scrambling block inputs

Table 5.1: analysis results for the bench mark circuit s38417

No of XOR gates	%HD	Power Dynamic(mw)	Cell leakage(uw)	Area overhead	Simulation time(us)
0	0	1.6254	82.0457	0	77.6
1	9.93	1.6468	82.0836	0.084	77.9
2	19.87	1.6502	82.0878	0.0988	77.9
3	29.93	1.6568	82.0976	0.108	78.4
4	39.85	1.6721	82.0986	0.124	78.4
5	49.67	1.6777	82.0994	0.1388	78.2
6	58.95	1.6940	82.1086	0.1609	78.4
7	68.94	1.7139	82.0873	0.175	78.2
8	79.85	1.7186	82.1113	0.1975	78.2
9	89.65	1.7228	82.1362	0.2125	78.2
10	99.54	1.7162	82.1105	0.228	78.2

Table 5.2: comparison of Hamming distance among three SST structures of S38417

No .of XOR gates	PUF-SST	SST	CSST
1	27.72	9.06	29.29
2	40.06	19.66	40.01
3	43.4	22.89	48.73
4	45.2	25.79	47.44
5	48.4	36.36	50.03
6	44.2	46.46	45.63
7	48.6	47.44	47.44
8	49.4	49.31	50.03

Table 5.3: comparison of hamming distance for different NSB

NSB	CSST	Proposed CSST
2	42.24	40.6
4	44.59	44.8
10	50.03	49.8

6. CHAPTER 6: PHYSICAL UNCLONABLE FUNCTION

6.1: INTRODUCTION

6.2: FEATURES OF PUF

6.3: TAXONOMY OF PUF

6.4: ARBITER PUF

6.1. INTRODUCTION:

Physical Unclonable Functions (PUFs) are a most reliable security functions used for storing authentication and cryptographic key. In general all the cryptographic keys and any information are stored in memories. But in recent years cloning and Reverse engineering methods like micro probing, power analysis, glitch attacks and laser cutting have become advanced and these allow the attacker to read the stored information in the device. To overcome these drawbacks Hardware intrinsic Security (HIS) is proposed to overcome these drawbacks and provide security. These security methods are based on the internal properties of the device.

PUFs are the kind that belongs to these HIS mechanisms. PUFs will generate the secret key based on the process variations that will occur during the fabrication of IC. When fabricating the ICs no two ICs can have the same properties, based on these properties PUF will generate a unique key. These properties mainly include gate delays, interconnect delays and threshold voltages. The inputs –outputs of PUF circuit are called challenge response pairs (CRPs). For each challenge PUF will give different responses. A device will have a unique response for the same challenge because of internal fabrication variability. These internal structure variations for any device are distinct, hidden and unique.

Based on the no of CRPs taken these PUFs are classified into two types 1) weak PUFs 2) strong PUFs. If a PUF supports less no of CRPs then it is weak PUF. These weak PUFs are used for low cost authentication purposes. If more no of CRPs are taken then those PUFs called strong PUFs.Applications of these strong PUFs are secured cryptographic public/private key generation methods and generation of Pseudo Random Functions.

6.2. FEATURES OF PUF:

Uniqueness: The ability of the PUF circuit to generate a unique response for a particular chip among the group of chips of the same type for same stimulus. Hamming distance is used to measure the uniqueness. Uniqueness is an estimate of an inter chip variation of a PUF response.

Reliability: Reliability of the PUF is the ability of a PUF circuit to generate the same response for a given challenge repeatedly applied. The ideal value of reliability of a PUF circuit is 100%. Environmental conditions like temperature, supply voltages and other issues like aging of the CMOS gates will affect the reliability of the PUF circuit.

Uniformity: The estimation of the proportion of 0's and 1's in the PUF response. For an ideal PUF, the value of uniformity is 50%. The Uniformity of a PUF is defined using a percentage of the hamming weight of the response.

Bit –aliasing: The PUF circuit in the different chips produces nearly identical responses which is an undesirable effect. Bit-aliasing of n^{th} bit in the PUF response is calculated as the percentage hamming weight of the n^{th} identifier across k (total) devices.

Among all the PUFs some PUFs will have some good features and another type PUFs will have some good features. So comparison of different features, among RO-PUF and Arbiter PUF [28] are shown in following table 6.1

Table 6.1: comparison of PUF features among RO-PUF and Arbiter PUF

	Ideal Value	Arbiter PUF	RO PUF
Uniqueness	50%	7.20%	47.24%
Reliability	100%	99.76%	99.14%
Uniformity	50%	55.69%	50.56%
Bit-aliasing	50%	19.57%	50.56%

6.3. TAXONOMY OF PUF:

Based on the usage of randomness introduction PUFs are classified as two types 1)

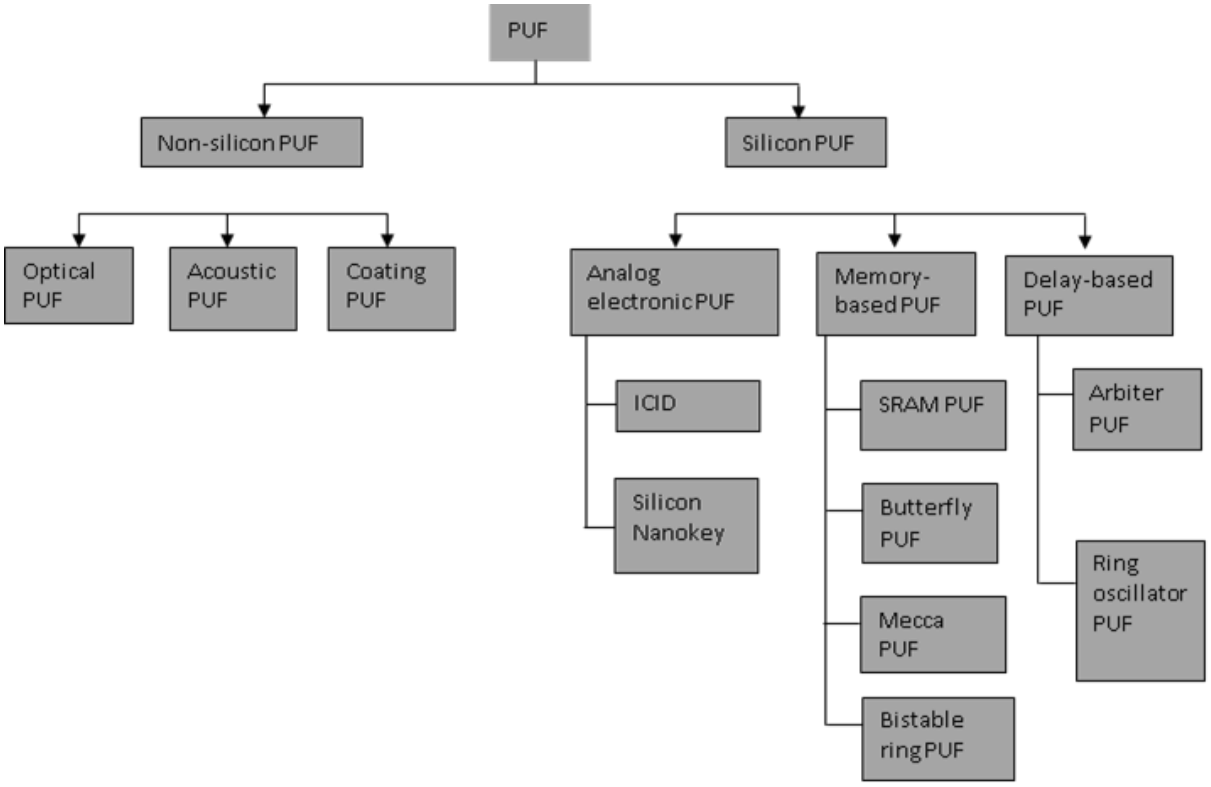


Fig 6.1: taxonomy of PUF [30]

Non-silicon PUF 2) silicon PUF. Non-silicon PUFs introduce randomness externally and silicon PUFs uses intrinsic randomness.

Brief introduction of all different PUFs is described below

Optical PUF: optical PUF is also known as POPWF (Physical One Way Functional). It was a transparent material which is doped with light scattering particles. When a laser beam fell on the transparent material, it will generate a random and unique pattern. The Position of the laser beam scattering on the material is an uncontrolled process. So it is very hard to design the PUF with the same characteristics. Therefore, these optical PUFs can't be cloned.

Coating PUF: This can be designed on the top layer of an IC. On the top of IC metal wires are laid

in comb shape. An opaque material is filled with dielectric material in the space between the top of the IC and comb structure. Due to the random placement, size and dielectric strength of the particles, in between the metal wires then there certainly exits capacitance.

SRAM PUF:SRAM PUF is a kind of memory based PUF. It uses the unpredictability of the starting value of volatile memory cells. This is caused due to the asymmetries in the memory cell routing, transistor characteristics.

Butterfly PUF: This is also one kind of memory based PUF, which is similar to SRAM PUF. It contains two memory cells whose start up value is very difficult to predict. In this Butterfly PUF all the SRAM cells are reset to unexpected state when it is reset.

Delay based PUFs:

Using the delays of the gates that are used in the Integrated Circuit, two types of PUFs are proposed.

1) Ring Oscillator PUF (RO-PUF) 2) Arbiter PUF

RO-PUF:

Ring oscillator is a circuit that is used to generate square wave by using odd no of inverters. Since the delay of each inverter is not same due to manufacturing variations, there will be differences in the frequencies. These square waves are given to counters, at a particular point of time we will compare the values in the counters. Based on the comparator values logic '1' or logic '0' is generated. Combination of such ring oscillators will give the required no of bits.

Block diagram of basic Ring Oscillator

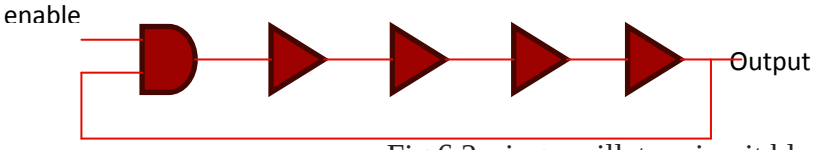


Fig 6.2: ring oscillator circuit block diagram

6.4. ARBITER PUF:

This PUF is also based on the delays of the connecting wires that are used in the circuits. Here a series of multiplexers are used, selection signals are used as challenge bits.

In this thesis, we had worked on Arbiter PUF that is used in the block diagram of PUF-based SST. Fig 6.3 shown below gives the block diagram of Arbiter PUF

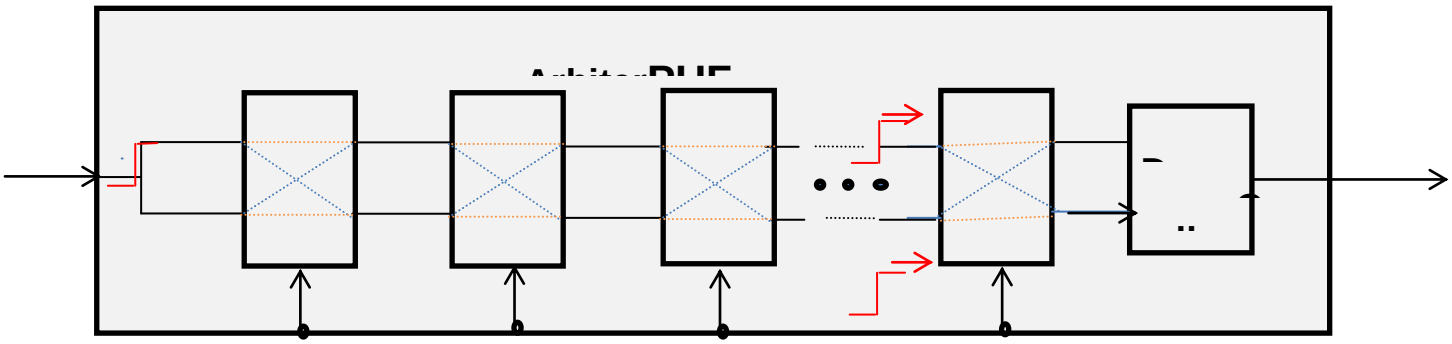


Fig 6.3: Block diagram of Arbiter PUF

Arbiter PUF contains a series of multiplexers and an Arbiter at the end of all the multiplexers to detect which came first. Here the delays are implemented in various ways. For example LUTs are used to implement extremely precise delay lines. Arbiter PUFs are good in terms of adhering to PUF properties. Here this Arbiter PUF is designed using Hardware Description Language (HDL) and implemented in FPGA Spartan-3E board.

Here we have calculated the Uniqeness of the PUF using some standard formula given by Maes and Verbauwhede.

$$U|C_1 = \frac{2}{k(k-1)} \sum_{i=1}^{i=k-1} \sum_{j=i+1}^{j=k} \frac{HD(R_i,R_j)}{m} \times 100\%$$

Where k referes to number of FPGAs used, m referes to number of bits generated by the PUF. Designed Arbiter PUF has uniqueness of approximately 39.52%. Ideal value of Uniqeness is 50%

7. CHAPTER 7: CONCLUSION AND FUTURE WORK

7.1: CONCLUSION

7.2: FUTURE WORK

7.1. CONCLUSION:

In this thesis, we are proposing a Novel PUF based SST. This method eliminates the drawbacks of Connecticut Secure Split Test (CSST) these are 1) use of memory devices which is vulnerable to reverse engineering. 2) Since only scan tests are used for testing the devices in previous methods, but in some cases, functional results are also needed so this method is proposing the design that is used for functional test also.

Use of this method will increase the security of design while testing that will counter the effects of counterfeits. To add different blocks additionally to the original circuit small area overhead is required. Hamming distance will increase if the number of scan chains in the DFT insertion for the design. This method requires 0.228% of area overhead.

7.2. FUTURE WORK:

Future work for this can do in the following direction.

Since this method is designed only for the assembly, in future we can implement this for the whole supply chain.

BIBLIOGRAPHY:

[1] J. Howard, "Fault Diagnosis Aware ATE Assisted Test Response Compaction," in the Asia South Pacific - Design Automation Conference, 2011.

[2] M. L. Bushnell and V. D. Agarwal, Essentials of Electronic Testing for Digital, Memory, and Mixed-Signal VLSI Circuits, New York: Springer, 2000.

[3] Z. Navabi, Digital System Test and Testable Design: Using HDL Models and Architectures, New York: Springer, 2011.

[4] Y. L. Sung-Mo Kang, CMOS Digital Integrated Circuits, and Boston: Tata McGraw Hill Education, 2003.

[5] "Reference Manual for Verigy 93000," [Online]. Available: www.advantest.com.

[6] "Synopsys On-Line Documentation (SOLD)," [Online]. Available: www. Synopsys.com.

[7]] B. Yang, K. Wu and R. Karri, "Secure scan: A Design-for-Test Architecture for Crypto Chips," *EEE Transaction on Computer-Aided Design for Integrated Circuits Systems*, vol. 25, no. 10, pp. 2287-2293, October 2006.

[8] Public-Key Cryptography and the RSAAlgorithmLecture Notes on “Computer and Network Security”by Avi Kak.

[9] Implementation of RSA Algorithm on FPGAAnkit Anand, Pushkar Praveen Centre for Development of Advanced Computing, (CDAC) Noida, India.

[10] VHDL for RSA Public Key System Engineering and Applied Science Memorial University of NewfoundlandbyRui He, Jie Gu, Liang Zhang, Cheng Li.

[11]Implementation of RSA CryptosystemUsing Verilog by Chiranth E, Chakravarthy H.V.A, Nagamohanareddy P, Umesh T.H, Chethan Kumar M.

[12] G. Contreras, M. T. Rahman, and M. Tehranipoor, "Secure Split-Test for Preventing IC Piracy by Untrusted Foundry and Assembly," in Int.Symposium on Defect and Fault Tolerance in VLSI Systems, 2013.

[13] MD. Tauhidur Rahman et al., "CSST: An Efficient Secure Split-Test for Preventing IC Piracy," In IEEE North Atlantic Test Workshop, May- 2014.

[14] MD. Tauhidur Rahman, Domenic Forte, Quihang Shi, Gustavo K. Contreras, and Mohammad Tehranipoor CSST: Preventing Distribution of Unlicensed and Rejected ICs by Untrusted Foundry and Assembly, International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT) -October- 2014.

[15] Rostami M, Koushanfar. F, Karri. R, "A Primer on Hardware Security: Models, Methods, and Metrics", *Proceedings of IEEE*, Vol. 102, Issue – 8, pp. 1283-1295, Aug 2014.

[16] U. Guin et al., "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," Journal of Electronic Testing, vol. 30, pp. 9-23, 2014.

[17] H. Livingston, "Avoiding Counterfeit Electronic Components", IEEE Transactions on Components and Packaging Technologies, vol. 30, pp. 187-189, 2007.

[18] "Defense Industrial Base Assessment: Counterfeit Electronics", http://, www.bis.doc.gov, U.S. Department of Commerce, Bureau of Industry and Security Office of Technology Evaluation, 2010.

[19] J. Stradley and D. Karraker, "The Electronic Part Supply Chain and Risks of Counterfeit Parts in Defense Applications", IEEE Transactions on Components and Packaging Technologies, vol. 29, num. 3, pp.703-705, 2000.

[20] K. Chatterjee and D. Das, "Semiconductor Manufacturers Efforts to Improve Trust in the Electronic Part Supply Chain", IEEE Transactions on Components and Packaging Technologies, vol. 30, num. 3, pp.547-549, 2007.

[21] Y.M. Alkabani and F. Koushanfar, ”Active hardware metering for intellectual property protection and security”, in proc. 16th USENIX Security Symposium, pp.20:1-20:16, 2007.

[22] J.A. Roy, F. Koushanfar, and I.L. Markov, ”EPIC: Ending Piracy of Integrated Circuits”, in proc. Design, Automation and Test in Europe 2008 (DATE ’08), pp.1069-1074, 2008.

[23] G.E. Suh and S. Devadas, ”Physical Unclonable Functions for Device Authentication and Secret Key Generation”, in proc. 44th ACM/IEEE Design Automation Conference (DAC ’07), pp.9-14, 2007.

[24] Jeroen Delvaux, Dawu Gu, Dries Schellekens, Ingrid Verbauwhede “Secure Lightweight Entity Authentication with Strong PUFs: Mission Impossible? “Lecture Notes in Computer Science, Volume 8731, pp 451-475, Cryptographic Hardware and Embedded Systems – CHES 2014.

[25] F. Koushanfar, G. Qu, M. Potkonjak, ”Intellectual Property Metering”, in proc. 4th International Workshop on Information Hiding (IHW ’01), pp.81-95, 2001.

[26] Majzoobi, Koushanfar, Potkoniak, “Techniques for Design and Implementation of Secure Reconfigurable PUFs”, ACM Transactions on Reconfigurable Technology and Systems (TRETS), Vol.2, Issue 1, Article No.5, March 2009.

[27] Abranil Maiti and P. Schaumont, "Improved Ring Oscillator PUF: An FPGA-Friendly Secure Primitive", *IACR Journal of Cryptology*, vol. 24, issue 2, April, 2011, pp. 375-397.

[28] Yamamoto, D.; Sakiyama, K.; Iwamoto, M.; Ohta, K.; Takenaka, M. & Itoh, K. “Variety enhancement of PUF responses using the locations of random outputting RS latches Journal of Cryptographic Engineering, Springer, Berlin Heidelberg, 2013, 3, 197-211.

[29] Sahoo, D.P.Saha,; Mukopadhyay, Chakraborty, “ Physically Unclonable Functions a promising security primitive for the internet of things”.

[30] M. Tehranipor,; Hardware security and trust, University of Connecticut.

[31] M. Rostami and F. Koushanfar,; Rice university: hardware security: threat models and metrics.

[32] F. Koushanfar, Rice university: A survey on Hardware metering.